REMARKS

In the office Action, the Examiner rejected claims 1-11 under 35 U.S.C. 102(e) as being anticipated by the Benson et al. (U.S. Patent 6,651,169) reference.

35 USC 102(e)

The Benson et. al. reference discloses a method by which a customer downloads a single piece of software from a server by a network (see column 5 lines 56-58). Therefore, the invention of Benson et. al. is primarily convenient to download single software programs which comprise only a limited data volume.

By contrast, Claim 1, as amended, describes a method to provide a storage medium containing a plurality of application programs to a user. Thus, the present invention is suitable to provide application programs which contain even large amounts of data, and which particularly comprise a plurality of programs which may interfere with each other but for the fact that each application program must be individually enabled by a respective comparison between the copy protection identification and the product identification.

In support of the claim 1 amendments, the specification describes a method wherein a user receives a plurality of user programs from the manufacturer of the user programs on a storage medium (page 5 lines 4-6). Further, the user, upon delivery of the user programs, can only enable tho user programs that the user had ordered and purchased (page 7 lines 15-17). When the user would like to purchase another user program at a later time, the only thing required to enable this newly purchased user program is a new product identification (page 7, lines 17-19).

In addition, the Benson et. al. disclosure is based on a functional relationship between the copy product identification, which is created by the installation program (nonce), and several public and private keys assigned to the customer and producer. On the other hand, claim 1, as amended, provides a method wherein the copy protection identification is directly connected to the user's data processing system as a hardware module, and is known by the software producer.

In support of the claim 1 amendments, the specification describes a method wherein the user receives a dongle from a manufacturer with a copy protection identification (page 5, lines 9-10). The dongle must be plugged onto the parallel interface of the data processing, thus directly connecting the copy protection identification to the user's data processing system (page 5 lines 10-11).

The Benson et al. reference also discloses a computer system containing a copy protection mechanism that requires the installation program itself, with no user input, to encrypt the product identification (generates a "nonce") during installation (see column 8, lines 7-13). Figure 3 (Box 31) denotes this process. This encryption step is necessary for the Benson et al. invention in order to verify that the user is licensed to use the protected software.

By contrast, claim 1, as amended, provides that a user receives from a producer an encrypted product identification. The user inputs the encrypted product identification during program installation. Therefore, the installation program itself performs no encryption, and so the Benson et al. reference does not anticipate the invention in claim 1.

In support of these claim 1 amendments, the specification describes a method wherein a product identification and a user identification are communicated to the user (page 3, lines 12-13; page 5 lines 13-15). Further, the producer defines the product identification, and provides the user with this product identification (page 8 lines 8-12). The product identification given to the user is in an encrypted form (page 3 line 14; page 5 line 15-17). The user inputs the encrypted product identification when prompted to do so by the installation program (page 5 lines 19-22). Moreover, the specification makes no reference to an installation program that encrypts a product identification (generates a"nonce").

The claims 2-11 depend from claim 1 and so the same comments apply.

Also, in the Benson et al. reference, the user, in order to enable the system, must insert a floppy disk that contains encrypted private information (see column 7 lines 10-20). The user must input a pass phrase in order to decrypt the floppy, thus requiring decryption at this initial step in installation.

New claim 12 describes a method by which the copy protection identification connected with the hardware module must coincide with characters input by a user at installation. However, no decryption takes place at this initial step in installation. Therefore, the Benson et al. invention does not anticipate the method of claim 12.

In support of new claim 12, the specification references a method wherein the installation program is loaded on a data processing system of the user and is started (page 5, lines 19-20). The installation program contains a menu prompt and asks for the input of the copy protection identification given to the user (page 5 lines 20-21). While the specification describes the product identification as encrypted, the specification fails to describe the copy protection identification given to the user as encrypted. Therefore, the copy protection identification given to the user is not encrypted. The installation program checks to see whether the copy protection identification input by the user coincides with the copy protection identification connected with the hardware module ("dongle") (page 5, lines 22-23; page 6, line 1). The specification makes no reference to a decryption at this initial step in installation.

Since claim 12 depends from claim 1, it distinguishes the entire invention described in claim 1 as compared to the copy protection system and method described in the Benson et al. reference.

Further amendments are made to claims 1 and 7 in order to provide antecedent basis for all claim terms.

Specification Changes

Changes to the specification are made in order to correct typographical errors in the original application.

Applicant respectfully submits that the respective copy protection identification might also be another hardware feature of the user's data processing system, for example a system specific-unique identification number, e.g. a Media Access Control number (MAC system address). Such control numbers are typically used for Ethernet or Token Ring computer

network adapters and mostly burned/stored inerasable in a memory of the adapter as a serial number.

Conclusion

Each issue has been addressed and so favorable reconsideration and allowance of the present application is hereby requested.

Respectfully submitted,

Melvin A. Robinson (Reg. No. 31,870)
Schiff Hardin LLP
Patent Department
6600 Sears Tower
Chicago, Illinois 60606
Telephone: 312-258-5785
CUSTOMER NO. 26574
ATTORNEY FOR APPLICANT

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail addressed to:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

on November 22, 2005.

CH1\ 4401524.2